I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

CARLA BULFORD*

Between East and West: The APEC Privacy Framework and the Balance of International Data Flows

Abstract: Although comprehensive privacy legislation has been in place in the European Union since 1995, the United States has continually declined to introduce similarly comprehensive privacy legislation. The Asia-Pacific Economic Cooperation ("APEC") has adopted a Privacy Framework that can be used both by member economies to adopt comprehensive privacy legislation and by industry groups and individual companies to implement self-regulatory standards. This note provides an overview of the APEC Framework and describes recent efforts implementing it, as well as a brief discussion of the Framework in relation to privacy regimes in the United States and Europe.

* Carla Bulford is a Juris Doctor candidate at The Ohio State University Moritz College of Law, class of 2008. I would like to thank Martha K. Landesberg for her invaluable guidance.

I. INTRODUCTION

In the Summer of 2006, the United States Department of Veterans Affairs ("VA") revealed that a computer containing the personal information of as many as 26.5 million veterans was missing.[1] This data breach briefly drew congressional attention to a small portion of a much larger matter: how to control and protect the massive amounts of digitized information that drive the modern global economy. The attention drawn by the VA's data security breach was a new high-water mark for public awareness of the risk to personal data that persists under the United States' piecemeal regulatory regime. Huge quantities of personal information are exchanged every day between companies domestically and internationally. Every border crossed by personally identifiable information, tangible or virtual, represents a potential risk to the integrity and security of that information, because every border represents a different degree of regulatory protection for that information. The European Union ("EU") codified its response to personal data privacy and security concerns over a decade ago, beginning with the Data Protection Directive of October 1995 and the individual member states' national laws implementing it.[2]

In the United States, the federal government has taken a sectoral approach, which addresses the protection of specific types of personal information through targeted laws, rather than implementing comprehensive privacy legislation. In 2004, the Asia-Pacific Economic Cooperation ("APEC"), of which the U.S. is a member, adopted a Privacy Framework for electronic commerce as a conceptual blueprint for comprehensive privacy legislation, self-regulatory standards, and individual business practices in APEC's twenty-one member states. Although member economies are not bound by the Framework, it serves as a unifying baseline for their privacy policies. This note begins by describing APEC and its role in Pacific-Rim trade. It continues with an overview of the APEC Privacy Framework ("Framework") and recent efforts to implement it, and concludes by

---

[1] David Stout & Tom Zeller, Jr., *Vast Data Cache about Veterans is Stolen*, N.Y. TIMES, May 23, 2006, http://www.nytimes.com/2006/05/23/washington/23identity.html?ex=1178769600&en=265fd0558da2f428&ei=5070.

[2] Council Directive (EC) 95/46, Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such, 1995 Official Journal of the European Communities (L 281) 31, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

briefly comparing the Framework with European and United States approaches to privacy legislation.

II. APEC HISTORY AND PURPOSE

APEC began as an informal meeting of government trade officials.[3] APEC's activities are strictly limited to the facilitation of economic development,[4] as is demonstrated by its "Three Pillars": "Trade and Investment Liberalisation, Business Facilitation, and Economic and Technical Cooperation."[5] Unlike other multinational regimes, such as the European Union or the General Agreement on Treaties and Trade ("GATT"), APEC does not require treaty obligations from its participants or in any way bind their behavior through its actions.[6]

APEC's function is to facilitate open communication among its member economies about matters that affect trade and investment in the Pacific Rim. To this end, APEC is designed to follow strictly democratic principles: all economies have an "equal say" and decisions are made by consensus.[7] APEC's emphasis on a nonbinding approach facilitates productive interactions among its member states by creating a less charged environment. Without the twin specters of treaty and pecuniary obligations, member economies are free to examine their interrelated economies with a view toward determining where improvement is needed and how it can be created. This

---

[3] Greg J. Bamber, *How is the Asia-Pacific Economic Cooperation (APEC) Forum Developing? Comparative Comments on APEC and Employment Relations*, 26 COMP. LAB. L. & POL'Y. J. 423, 429 (2005).

[4] APEC's economic limitation has garnered the organization some criticism when contrasted with European organizations, such as the European Union or the Council of Europe, which have cultural or humanitarian missions in addition to their economic agendas. ASEM, the Asia-Europe Meeting, is sometimes identified as an organization with greater potential to create change in Asia. *See, e.g.*, Simone McCormick, Note, *ASEM: A Promising Attempt to Overcome Protective Regionalism and Facilitate the Globalization of Trade*, 10 ANN. SURV. INT'L & COMP. L. 233 (2004). At the same time, APEC has escaped the criticism that has been leveled at the EU for its "inhibiting" effect on globalization. *Id.* at 244–45.

[5] APEC AT A GLANCE, APEC SECRETARIAT, APEC#205-SE-05.2, 5 (2005), *available at* http://www.apecsec.org.sg/apec/publications/free_downloads/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/sec/pubs/2005.Par.0005.File.v1.1.

[6] *Id.* at 2.

[7] *Id.*

arrangement is particularly valuable for members with developing economies, because the majority of APEC's activities outside its yearly summits are workshops and studies focused on issues relevant to the relationship between regulation and growth.

APEC's concrete achievements during its seventeen-year history are in two areas. The first of these is conceptual. In 1994, APEC adopted the Bogor Goals, which set the two-tiered aim of "free and open trade and investment in the Asia-Pacific by 2010 for developed economies and by 2020 for developing economies."[8] In 1995, APEC adopted the Osaka Action Agenda ("OAA"), "which provided a framework for meeting the Bogor Goals through trade and investment liberalisation, business facilitation and sectoral activities, underpinned by policy dialogues, economic and technical cooperation."[9] While the goals and the action agenda are voluntary, each economy is responsible for creating and implementing an Individual Action Plan ("IAP") identifying the concrete steps that it will take to achieve the Bogor goals.[10] The second area of achievement is at the practical level. This area is demonstrated by the breadth and number of completed APEC projects, which range from workshops on human resource issues or securities regulation to studies of labor markets and educational technology,[11] as well as the APEC card, which provides

---

[8] APEC, Key APEC Milestones, http://www.apec.org/apec/about_apec/history.html (last visited Feb. 6, 2008).

[9] *Id.*

[10] *FTAs: Working Towards Bogor Goals*, APEC E-NEWSLETTER, Aug. 2004, http://www.apec.org/apec/enewsletter/aug_vol3/onlinenewsa.html. The contents of the APEC IAPs are specified by the APEC IAP Format Guidelines, which were established in 2000 and revised following changes made to the OAA in 2001 and 2002. The APEC IAPs provide a clear overview of each member economy's regulation of trade, investment, commercial activity and arbitration. The IAPs are invaluable for two reasons. First, IAPs admirably serve their stated goal of transparency due to their completeness and uniform elements. The uniformity allows quick and meaningful comparisons between the member economies. Second, the IAP guidelines specify the provisions that comprehensive trade and business legislation should include. The guidelines provide a quasi-legislative roadmap for developing countries to consider as they adapt their domestic regulatory regimes to facilitate their development goals.

[11] APEC Project Database, List of APEC Projects, http://203.127.220.68/Apecp1.nsf/$$SearchTemplateDeFaultV/2B4CDC411BFF760F48257234007002FC?openDocument (last visited Feb. 6, 2008).

frequent business travelers with visa-less access and a fast-track through customs in fourteen of the APEC member economies.[12]

III. THE APEC PRIVACY FRAMEWORK

The APEC Privacy Framework is organized in four parts: Preamble, Scope, APEC Privacy Principles, and Implementation. It includes both text and commentary.[13] The Framework was written by APEC's Electronic Commerce Steering Group ("ECSG"), and was adopted at the 16th APEC Ministerial Meeting in Santiago, Chile, in 2004.[14] Taken as a whole, the Framework has four objectives:

1. to develop appropriate privacy protections for personal information;

2. to prevent the creation of unnecessary barriers to information flows;

3. to enable multinational businesses to implement uniform approaches to the collection, use, and processing of data; and

4. to facilitate both domestic and international efforts to promote and enforce information privacy protections.[15]

The Framework Principles are largely based upon the Organisation for Economic Co-operation and Development's ("OECD") 1980 *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data* ("OECD Guidelines").[16]

---

[12] APEC, APEC Business Travel Card, http://www.apec.org/apec/business_resources/apec_business_travel0.html (last visited Feb. 6, 2008).

[13] APEC SECRETARIAT, APEC PRIVACY FRAMEWORK (2005), *available at* http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf.

[14] News Release, APEC Electronic Commerce Steering Committee, Seminar Highlights the Business Benefits of Increased Protection of Data, (Sept. 8, 2005), http://www.apec.org/apec/news___media/2005_media_releases/080905_ecsgsomiii.html.

[15] APEC, Electronic Commerce Steering Group, http://www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.html (last visited Feb. 6, 2008).

[16] *APEC Online Privacy Protection Framework to Facilitate Increased Electronic Commerce*, APEC E-NEWSLETTER, Mar. 2004, http://www.apec.org/apec/enewsletter/march_vol2/

A. SCOPE AND APPLICATION

The Framework sets out guidelines for the collection, use and sharing of "personal information" by "personal information controllers." "Personal information" is defined as "any information about an identified or identifiable person."[17] The Commentary states that "personal information" also includes information that, while not capable of identifying an individual on its own, would do so if "put together with other information."[18] Arguably, the breadth of the definition could encompass truncated account numbers and encrypted identifiers, which are rendered intelligible by the application of an algorithm. It could also apply to biometric information such as blood type, DNA analysis, or fingerprints, if such information could be tied to numeric or personal identifiers.

The Framework distinguishes "personal information," which is governed by the APEC Privacy Principles, from "publicly available information," which is not.[19] The Commentary explains that the Framework's Notice and Choice Principles have limited applicability when information is in the public domain. An information controller is able to obtain information in the public domain without contacting the data subject. This acknowledgement indicates that information obtained from publicly available government records, for example, voter registration and print or broadcast news, can be treated differently under the Framework than other personally identifiable information, provided that the former is used alone and not put together with personal information that is not publicly available.

---

onlinenewse.html#. In September 1980, the Organization released its *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, Sept. 23, 1980, http://webdomino1.oecd.org/horizontal/oecdacts.nsf/linkto/C(80)58. The instrument specified that its eight Guidelines should be regarded as minimum standards that individual member states could augment as needed to protect privacy and personal liberty. *Id.* The Guidelines address: collection limitations, data quality, purpose specifications, use limitations, security safeguards, openness, individual participation, and accountability. *Id.*

[17] APEC Privacy Framework, *supra* note 13, § 10. The Commentary specifies that the Framework applies to natural, living, persons, but "not legal persons," which specifically excludes corporations and other legal entities from the protection extended by the framework.

[18] *Id.* § 9.

[19] *Id.* § 11. The Framework defines "publicly available information" as personal information about an individual that "the individual knowingly makes or permits to be made available to the public, or [information that] is legally obtained and accessed from a) government records that are available to the public; b) journalistic reports; or c) information required by law to be available to the public." *Id.*

The Framework defines "personal information controller" as "a person or organization who controls the collection, holding, processing or use of personal information."[20] The definition specifically includes a person or organization that instructs another person or organization to collect, hold, and process personal information. It excludes persons who collect, hold, or process information under the instruction of another and persons who do so in connection with the person's own personal, family, or household affairs. Thus, under the Framework, entities are responsible for the actions of agents who collect, hold, use, process, transfer, or disclose information on their behalf.[21]

As noted above, the Framework, unlike the EU Data Protection Directive, is not binding upon APEC economies and does not confer individual rights to information privacy. The Framework explicitly contemplates that member economies will vary their implementation of the Principles, based upon "differences in [their] social, cultural, economic, and legal backgrounds."[22] Compatibility among member economies' privacy regimes is, however, essential to the facilitation of international commerce. Therefore, the Framework specifies that any exception to its Principles, including exceptions relating to national sovereignty, national security, public safety or public policy, should be "limited and proportional to meeting the objectives to which the exceptions relate" and publicly disclosed or made in accordance with law.[23]

B. THE FRAMEWORK'S PRIVACY PRINCIPLES

1. PREVENTING HARM

This Principle specifies that the privacy measures implemented by member economies should be aimed at preventing *misuse* of personal information.[24] Privacy protections implemented under the Framework "should be designed to prevent harm resulting from wrongful collection and misuse of personal information." Remedies for privacy

---

[20] *Id.* § 10.

[21] *Id.* § 10 Commentary.

[22] *Id.* § 10.

[23] *Id.* § 13.

[24] *Id.* § 14.

infringement should be "designed to prevent harms resulting from the wrongful collection or misuse of personal information, and should be proportionate to the likelihood and severity of any harm threatened by the collection or use of personal information."[25] This non-regulatory, harm-based approach distinguishes the Framework's focus from that of the EU Data Protection Directive and the national laws implementing it, which protect individual privacy as a fundamental right, and regulate the collection, use, disclosure and other processing of personal data accordingly.

2. NOTICE

The primary concern addressed by the Notice Principle is that individuals are informed a) that information is being collected, b) why the information is being collected, and c) how individuals may limit the use and disclosure of personal information. This Principle requires "clear and easily accessible statements about practices and policies with respect to personal information."[26] Such a statement must include:

1. the fact that information is being collected;
2. the purpose for which it is collected;
3. to whom the information may be disclosed;
4. the identity, location, and contact information of the personal information controller;
5. the choices the personal information controller offers individuals to limit the use and disclosure of their information; and
6. the choices the personal information controller offers for accessing and correcting . . . personal information.[27]

---

[25] *Id.* § 14 Commentary.

[26] *Id.* § 15.

[27] *Id.* § 15 (a)–(e).

This Principle specifies that requisite notice may be provided either before collection, at the time of collection, or as soon as is reasonably practicable. These options are consistent with the Framework's focus on facilitating regional commerce.[28] In determining when and how they will provide notice explaining their information practices, businesses must consider both their method of collection and the nature of the source used to obtain information. Clarity and accessibility of notice should be the guiding principles in members' notification requirements. The Commentary expresses an expectation that the most common method of notification will be a notice posted on the controller's Web site.[29] As is discussed in more detail below, the Framework requires that the information controller explain to the information subject the choices that allow him or her to limit the collection, use, and disclosure of his or her personally identifiable information. The Framework does not, however, specify the options that "should" be provided.

3. LIMITED COLLECTION

Following the OECD *Guidelines*, the Principle of Limited Collection requires that information collected be limited to information "relevant to the purposes of collection" that has been "obtained by lawful and fair means."[30] The Commentary takes a flexible approach to the determination of "relevance," and recognizes that it is not always appropriate to provide notice or obtain consent for the collection of personal information, for example, when such information is urgently needed in the event of a public health crisis or a security-related matter.[31]

---

[28] *Id.* § 16. The Commentary for this section specifies that instances where immediate notice is not practicable include instances of "electronic technology automatically collect[ing] information when a prospective customer initiates contact, as is often the case with cookies," and information that is obtained from a third party (for example when an insurance company obtains employee information from the employer for health insurance purposes). Alternatively, notice is not necessary if the information in question is publicly available or comprises business contact information, whether obtained from the individual, a public record.

[29] *Id.* §§ 15–17 Commentary.

[30] *Id.* § 18.

[31] *Id.* § 18 Commentary.

4. USES OF PERSONAL INFORMATION

The Framework's Use Principle specifies that personal information should be used "only to fulfill the purposes of collection and other compatible or related purposes," except when it is used: [32]

1. with the consent of the individual whose information is collected;

2. when the use is necessary to provide a product or service requested by the individual; or

3. under legal authority.[33]

The second exception, for "necessary use," is built upon the idea of implied consent arising out of an established business relationship. Once a relationship has been established between the collector and the individual, consent may be extended by implication due to a course of dealing. Although this established relationship exception may be necessary to sustain the current pace of business, it also raises concerns because the individual involved may not realize that that the information controller has no obligation to inform him about the continued use or exchange of information.

The Commentary contains several examples that expand upon the meaning assigned to "compatible or related purpose," including the "creation and use of a centralized database to manage personnel," "the processing of employee payrolls by a third party," or the "use of information collected by an organization for the purpose of granting credit for the subsequent purpose of collecting a debt owed to the organization." Other possibilities could include the use of a repeat customer's purchasing and browsing habits to make product recommendations.

5. CHOICE

When the actions of an information controller do not fall within the exceptions provided for compatible or related purposes and are subject to notice and choice requirements, the Framework requires that

---

[32] *Id.* § 19.

[33] *Id.*

statements notifying individuals of their choices be "clear [and] easily understandable," and that the mechanisms available be "accessible and affordable."[34] The choices offered and mechanisms provided must allow individuals to exercise control over the "collection, use, transfer and disclosure of their personal information."[35] The central concern identified in the commentary for this section is the need to allow individuals the choice of whether the "collection, use, transfer, and disclosure of their personally identifiable information"[36] is allowed. The Framework specifies neither the means of notification, nor the type of choice mechanism. The overarching intent of the Framework with regard to choice, indicated by the selective emphasis on personal choice and the nature of the caveats discussed above, is to inform consumers of data practices rather than to provide them a broad measure of control over the use of their information. The Framework is clearly intended to facilitate (or at the very least not to hamper) "necessary" business operations.

6. INTEGRITY OF PERSONAL INFORMATION

The Integrity Principle is a straightforward affirmation of the need for accurate information. Accuracy includes the need for information to be complete and up to date "to the extent necessary for the purposes of use."[37] The Commentary acknowledges that inaccurate or incomplete information may not be in the interest of either individuals or organizations.[38]

7. SECURITY SAFEGUARDS

The Security Principle identifies the need for the information controller to secure information once obtained, but does not specify the nature or means of that protection. This is, in part, a sound policy decision; technology-specific legislation manufactures its own obsolescence. In keeping with the Framework's harm-based, non-

---

[34] *Id.* §§ 19–20.

[35] *Id.*

[36] *Id.* § 20 Commentary.

[37] *Id.* § 21.

[38] *Id.* § 21 Commentary.

regulatory approach, the standard intended under this Principle is flexible: "[security] safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held."[39] The Principle also calls for periodic "review and reassessment" of the implemented safeguards, which serves to address the reality of rapidly changing security technology.[40] The Commentary limits the scope of security safeguards to those that are "*reasonable.*"[41] The reasonableness standard furthers the intent to maintain maximum flexibility in regulations established by member economies, or in self-regulatory rules established under the Framework.

8. ACCESS AND CORRECTION

The Access Principle states that individuals should have some means to access, correct, and even delete information about them that is held by a personal information controller.[42] Access is to be provided in a reasonable time, in an understandable format, and at a reasonable cost, if any, to the individual.[43] However, the Framework does not provide an absolute right of access to personal information. Access need not be provided, for example, if it would impose a burden or expense disproportionate to the privacy risk that might result from denying access, or would pose a risk to the security of confidential commercial information of persons other than the data subject. If an individual's access request is denied, this Principle provides that the

---

[39] *Id.* § 22.

[40] *Id.*

[41] *Id.* § 22 Commentary (emphasis added).

[42] *Id.* §§ 23–25 Commentary.

[43] *Id.* Providing the information in a "reasonable manner" includes a requirement that "normal methods" of interaction between organizations and individuals be used. "Normal methods" may include use of the individual's email, if email is a method that has been used for communication between the individual and the organization in question. Providing information in an "understandable form" does not preclude controllers from charging an individual for translation of the information provided. While an explanation of codes used by the organization should be provided, the obligation to render the information in a readily comprehensible format does not extend to converting computer code into text.

individual should receive an explanation of and instructions about how to challenge the denial.[44]

9. ACCOUNTABILITY

The Accountability Principle addresses transfers of personal information by the personal information controller. It holds controllers accountable not only for the specific measures they take to comply with the Framework Principles, but also for the information practices of data recipients, unless individual consent is obtained for the transfer.[45] In the absence of consent, the controller must "exercise due diligence and take reasonable steps to ensure that the recipient . . . will protect the information consistently with [the Framework] Principles."[46] Australian Attorney General Philip Ruddock identified the idea that accountability runs with the information as a "key feature of the Framework."[47]

The Framework's approach to transfers of personal information is in marked contrast to that of the EU Data Protection Directive, which, subject to exceptions including obtaining unambiguous consent, prohibits transfers to a country outside the EU unless that country "ensures an adequate level of protection" for the data.[48] The

---

[44] *Id.* § 25; *see id.* §§ 23–25 Commentary (access is limited by "what would be considered reasonable in the provision of access." This limitation is further qualified by another set of conditions on "what is to be considered reasonable in each of these areas," which includes "the nature of the information processing activity" as well as the nature of the information itself. Specifically, "confidential commercial information" should, under the wording of this principle, be accorded special protection that extends to the denial of access and correction rights to the individual to whom the information relates. "Confidential commercial information" is defined in §§ 23–25 Commentary as "information that an organization has taken steps to protect from disclosure, where such disclosure would facilitate a competitor in the market to use or exploit the information against the business interest of the organization causing significant financial loss.").

[45] *Id.* § 26.

[46] *Id.*

[47] APEC, News Photos, Attorney-General Philip Ruddock at the APEC Data Privacy Seminar on the International Implementation of the APEC Privacy Framework, (Jan. 22, 2007), http://www.apec.org/apec/news___media/2007_webcast/220106_aus_agruddockphotos.html (provides a link to the webcast of Mr. Ruddock's address).

[48] Council Directive (EC) 95/46, *supra* note 2, art. 25 (the derogations are set out in Article 26); *see* Export.gov, Safe Harbor Overview, http://www.export.gov/safeharbor/SH_Overview.asp (the details of the Safe Harbor) (last visited Feb. 6, 2008). Concerns that implementation of the Directive would result in a

Accountability Principle is intended to effectuate, rather than limit, both domestic and international transfers of personal data, as long as they are consistent with the Framework Principles.

C. SELF-REGULATORY EFFORTS UNDER THE FRAMEWORK

Consistent with its twin objectives of enhancing privacy protection and facilitating data flows within APEC, the Framework includes guidance on international implementation of the nine APEC Privacy Principles.[49] The guidance explicitly contemplates that member economies will support self-regulatory efforts to create cross-border privacy rules that are consistent with the Principles and mutually-recognized across member economies.[50] In 2005, several APEC economies, including the United States, formed the Cross Border Rules Study Group, as a subcommittee of the ECSG, to explore alternatives for developing cross-border privacy rules. The Group surveyed member economies' views on the implementation of cross-border rules, and presented its findings in January 2007.[51] In June 2007, twelve member economies agreed to support a "Data Privacy Pathfinder," or pilot project, to test a system of voluntary cross-border privacy rules. The Pathfinder is a public sector/private sector effort led in the U.S. by the Department of Commerce and based, in part, upon mutual recognition of public and private-sector certification

---

catastrophic suspension of transactions between EU member countries and the United States prompted the negotiation of the EU-US Safe Harbor agreement, which is administered by the U.S. Department of Commerce. The Safe Harbor includes Privacy Principles with which businesses voluntarily comply. Compliance permits the transfer of personal data collected in the EU to the United States. The Safe Harbor requires companies to publicly state their adherence to the Principles. Non-compliance subjects companies to enforcement action by the FTC or the Department of Transportation, rather than to the jurisdiction of EU data protection authorities. The details of the Safe Harbor are available at Export.gov, Welcome to Safe Harbor, http://www.export.gov/safeharbor (last visited Feb. 6, 2008); *see* Steven A. Wells et al., *[Un]Safe Harbor: No Common Denominator In Privacy Compliance*, 9 COMP. L. REV. & TECH J. 257, 261 (2004) ("[T]he benefits to the participating company include: the EU Commission finding that the Safe Harbor program provides adequate protection, automatic approval or waiver of prior approval requirements by member states for data transfer, actions against the company by EU citizens will be heard in the U.S., and no interruption of data flows.").

[49] APEC Privacy Framework, *supra* note 13, §§ 40–48.

[50] *Id.* §§ 46–48.

[51] U.S. Dep't of Commerce, A History of the ECSG in Brief (2007) (provided to the author for public use by U.S. Department of Commerce staff in August 2007).

authorities, or "accountability agents," that certify companies' adherence to the APEC Principles. Accountability agents, and even individual companies, may have their own internal rules, as long as they are consistent with the Principles. Data transfers are consistent with the Framework if all parties to a data transfer are certified. The Pathfinder project is expected to commence in 2008.[52]

D. IMPLICATIONS OF THE FRAMEWORK

The Framework is best interpreted as a reasonable indication of the concerns that privacy policy on the Pacific Rim will address. Unlike the EU Data Protection Directive, the Framework is not a binding set of minimum standards to which member economies must adhere. The Framework has no legislative timeline nor does it create a penalty for non-compliance. Although the Privacy Framework has been adopted by APEC in principle, it will not be fully implemented until all member economies have implemented privacy policies built around its Principles. The form of the individual legislation may vary widely.[53]

APEC's adoption of the OECD Principles is evidence of the enduring value of those Principles as a yardstick for privacy policy.

---

[52] In 2006, the OECD compiled and released a report on cross-border enforcement of privacy laws. *See* ORG. FOR ECON. CO-OPERATION AND DEV., REPORT ON THE CROSS-BORDER ENFORCEMENT OF PRIVACY LAWS (2006), *available at* http://www.oecd.org/dataoecd/17/43/37558845.pdf. The report affirmed the continued relevance of the OECD's 1980 principles and emphasized a continuing need for effective privacy legislation in the modern environment, because information "flows more freely, knows fewer national attachments, and indeed represents one of the significant forces behind the processes of globalisation." *Id.* at 7 (quoting COLIN BENNETT & CHARLES RAAB, THE GOVERNANCE OF PRIVACY, at xvi (1996)). Significantly, the report identified a distinct area of diversity in the implementation of privacy legislation among the states that returned the OECD's questionnaire: enforcement authority and enforceable remedies. The differences are interesting because both the majority of the survey respondents and the majority of OECD members are bound either by EU Directive 95/46/EC or Convention 108 through their membership in the EU or the European Economic Area ("EEA") and the Council of Europe. *See*, COUNCIL OF EUROPE COMM. OF MINISTERS, AMENDMENTS TO THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (1999), *available at* http://www.coe.int/T/E/Legal_affairs/Legal_cooperation/Data_protection/Documents/International_legal_instruments/Amendements%20to%20the%20Convention%20108.asp. However, the OECD report concludes, it is not "obvious . . . that in practice this diversity creates a barrier to enforcement co-operation." ORG. FOR ECON. CO-OPERATION AND DEV., *supra* note 52, at 12.

[53] *See, e.g.*, Rudy Guyon, *Outline of Privacy and Spam Laws in Japan and Australia (From a Company Perspective) and APEC Privacy Framework Brief Overview*, 865 PLI/Pat 595, 616 (June/July 2006).

The APEC Privacy Principles establish a conceptual paradigm for considering the regulatory issues that surround personal privacy. The intended purpose of the APEC Framework, however, is to permit implementation of the Principles in a manner that effectuates privacy protection in commerce without deeming privacy an absolute right.

IV. DISCUSSION

"Privacy" is a cultural concept. In Japanese, the words approximating "public" and "private" do not carry the same connotations that they do in English. Subtleties of usage in English itself differ, as well, between English-speaking countries. Ideas of what constitutes, or is acceptable in, public and private spaces vary widely from country to country. These cultural attitudes are informed and shaped by history; citizens of Russia, France or Germany, for example, may have an enhanced sensitivity to government access to and collection of personal details. This point suggests one possible motivation behind the protective "opt-in" requirements of EU Directive 95. As the author notes, the EU data-protection regime "vigorously defends the privacy of an individual's personal information[,] from both the government and the private sector, largely as a result of the region's grisly past."[54] Without memories and cultural attitudes that may drive the European approach, national-level authorities in the United States have taken a different approach to privacy regulation.

The reticence of the U.S. Congress to pass comprehensive legislation further illustrates this country's *laissez faire* stance. Generally speaking, "the market" is the laboratory in which approaches to privacy regulation develop and proliferate until they either succeed or fail. Frequently, state entities intervene to set legal parameters only after an innovation or practice has dramatically succeeded or failed. The APEC Privacy Framework falls between the U.S. and European approaches with a relatively hands-off approach that incorporates elements of the more proactive European model in a permissive set of Principles.

V. CONCLUSION

The United States and Europe currently represent opposite ends of the personal privacy spectrum. In the United States, legislation is

---

[54] *Id.* at 359.

concentrated in discrete areas where industry activity requires intensive use of personal data, for example, the Fair Credit Reporting Act[55] and Title V of the Gramm-Leach-Bliley Act,[56] or where a specific social concern is implicated, such as children's online privacy.[57] In contrast, the European approach, as defined by the EU Data Protection Directive, establishes a broad legislative baseline that applies whenever personal data is processed in the private sector.

Most importantly, the EU Directive restricts the transfer or transmission of data from the EU to any country whose privacy protections do not meet the Directive's "adequacy" standard. The APEC Privacy Framework does not include such a prohibition. In contrast to the reactive and industry-specific approach in the United States, the Framework is a comprehensive and theoretically coherent approach to privacy legislation and voluntary business practice.[58] The Framework can be described as a "multi-national friendly counterweight to strong central legislation under the EU Data Protection Directive,"[59] because it balances baseline privacy principles with wide latitude for economy-specific implementation.[60] From a

---

[55] *See* 15 U.S.C. § 1681 *et seq.* The legislation was passed in response to the inaccuracies and injustices that were revealed when credit bureaus' concerns that had previously been primarily local or regional were nationalized. It requires, for example, that the information contained in credit materials be both accurate and directly related to the purpose of evaluating credit-worthiness; prior to that time such reports may have contained purely anecdotal information frequently prejudicial in nature.

[56] 15 U.S.C. §§ 6801–09 (1999).

[57] *See, e.g.,* Children's Online Privacy Protection Act of 1998 ("COPPA"), Pub. L. No. 105-277, 112 Stat. 2681 (codified at 15 U.S.C. §§ 6501 *et seq* (2000)) (regulates the activities of Internet website operators in relation to information obtained online from children under the age of thirteen).

[58] *See, e.g.,* Ryan Moshell, Note, . . . *And Then There Was One: the Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 362 (2005); *see also* PAULA J. BRUENING, CONSUMER PRIVACY IN THE ELECTRONIC MARKETPLACE (2001) *available at* http://www.cdt.org/publications/consumerprivacy.pdf.

[59] Guyon, *supra* note 53, at 616.

[60] *See generally, id.* (providing an overview of Australian and Japanese privacy legislation). Both countries are APEC members that have laws "generally consistent with APEC," but those laws are at the same time "quite different from one another." Some differences between the two countries include: Australia has a single privacy commissioner, Japan spreads regulatory and enforcement powers between a number of agencies; Japan does not regulate international transfers (but instead makes the transferor responsible for the data it transfers), in contrast, Australia specifies the circumstances in which transfer is allowed (an approach that

policy standpoint, by establishing over-arching Principles that are not tied to particular types or uses of personal data, the Framework avoids some of the efficiency concerns raised by the strict application of the Directive and addresses the privacy concerns raised by inconsistencies in U.S. legislation that result from the piecemeal manner in which it is created.

Legislation grounded in common principles provides a predictable and stable business environment, which benefits both industry and individuals. Corporations that deal in personal, non-public information can tailor their internal policies around the same principles that will control new policy, and will benefit from increased consumer confidence. Predictability reduces compliance concerns and streamlines the legislative process by setting uniform parameters for legislative activity. Consumers benefit from a framework that places informed consent at the center of every policy decision, because it encourages accurate disclosure from companies that manipulate consumer data. The APEC Privacy Framework has the potential to provide these benefits to both domestic and international industry participants by establishing baseline principles without unnecessarily restricting the flow of information they protect. By establishing a practical middle ground, the Framework has the potential to force a broader compromise between the two ends of the spectrum. If enough countries adopt the flexible approach advocated in the Framework, EU member states will have to choose between re-evaluating their privacy standards and isolating themselves from the rest of the world.

---

echoes the EU's, but with more liberal standards); the definition of personal data in Japan includes more types of information than its counterpart in Australia. These differences demonstrate flexibility that is the strength of the APEC Framework. *Id.* at 617.